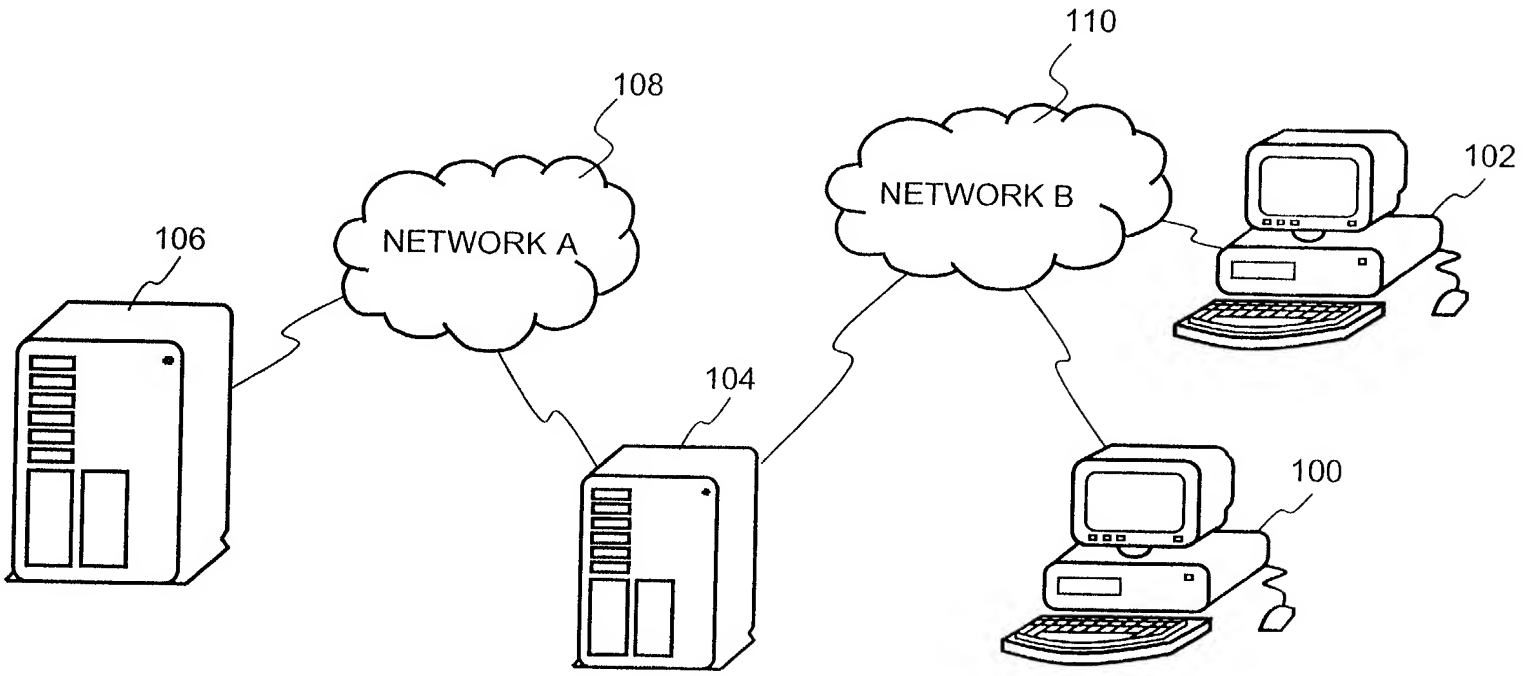


FIG. 1A

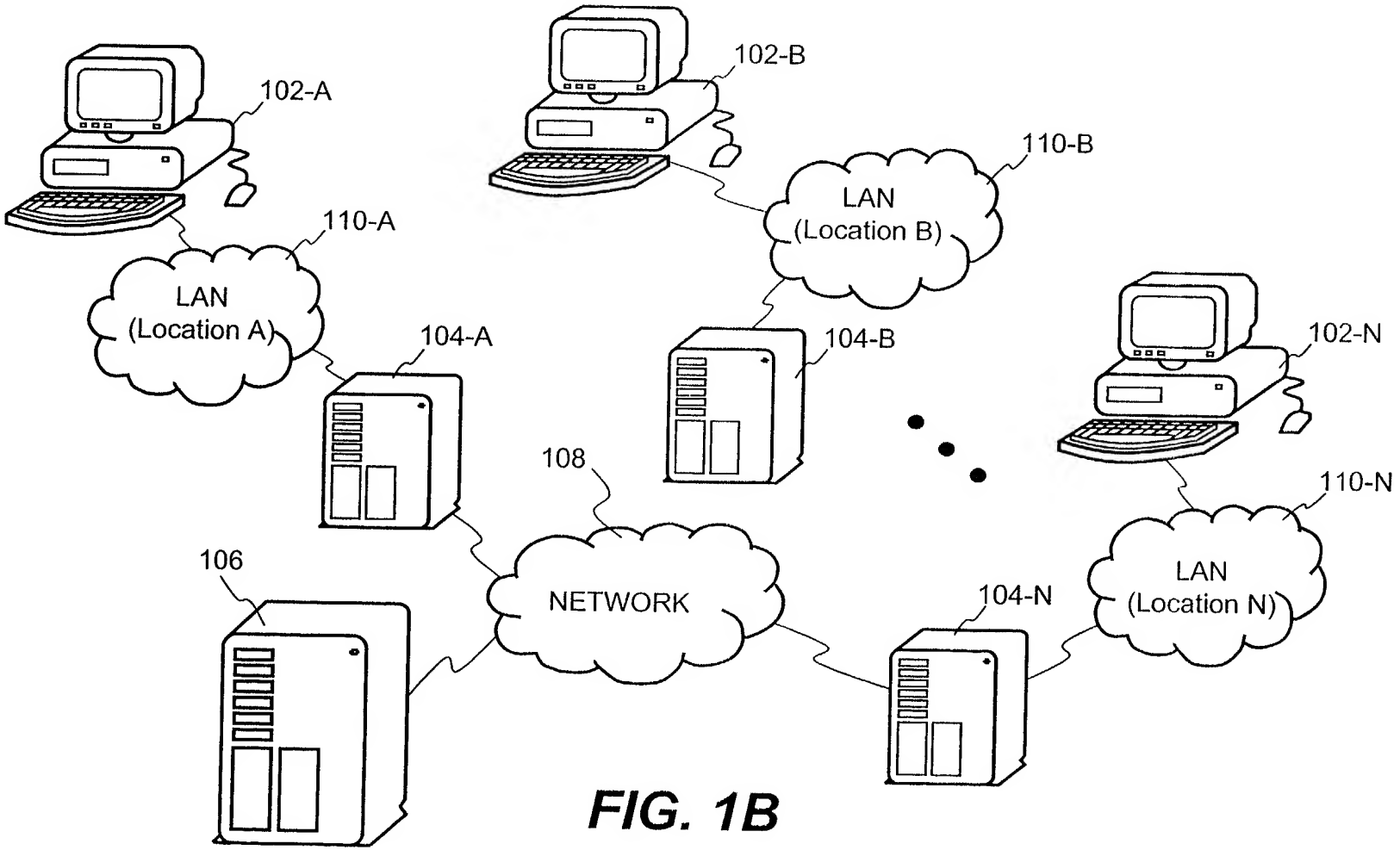

102-A
102-B
110-B
LAN
(Location B)
110-A
LAN
(Location A)
104-A
104-B
102-N
108
110-N
106
NETWORK
104-N
LAN
(Location N)

FIG. 1B

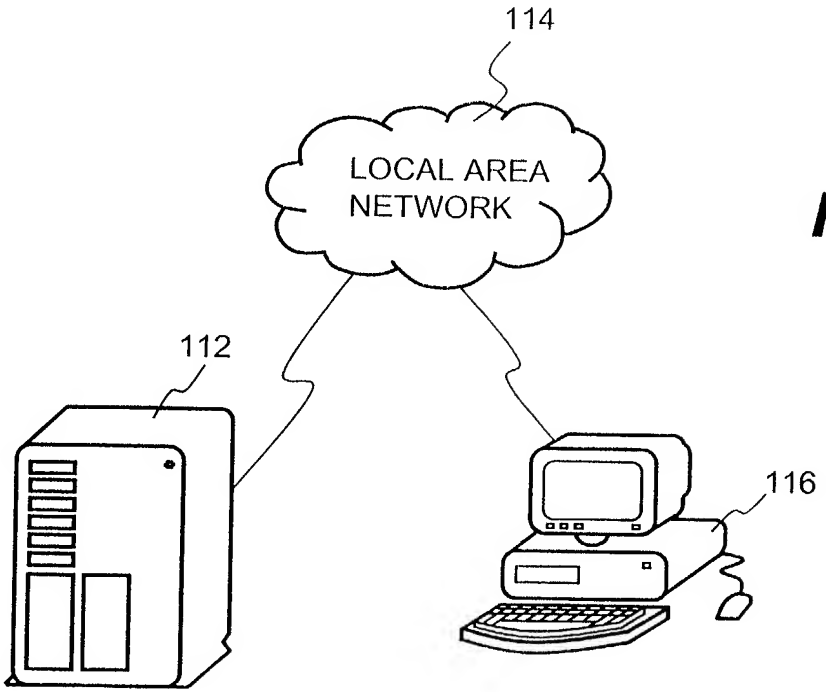


FIG. 1C

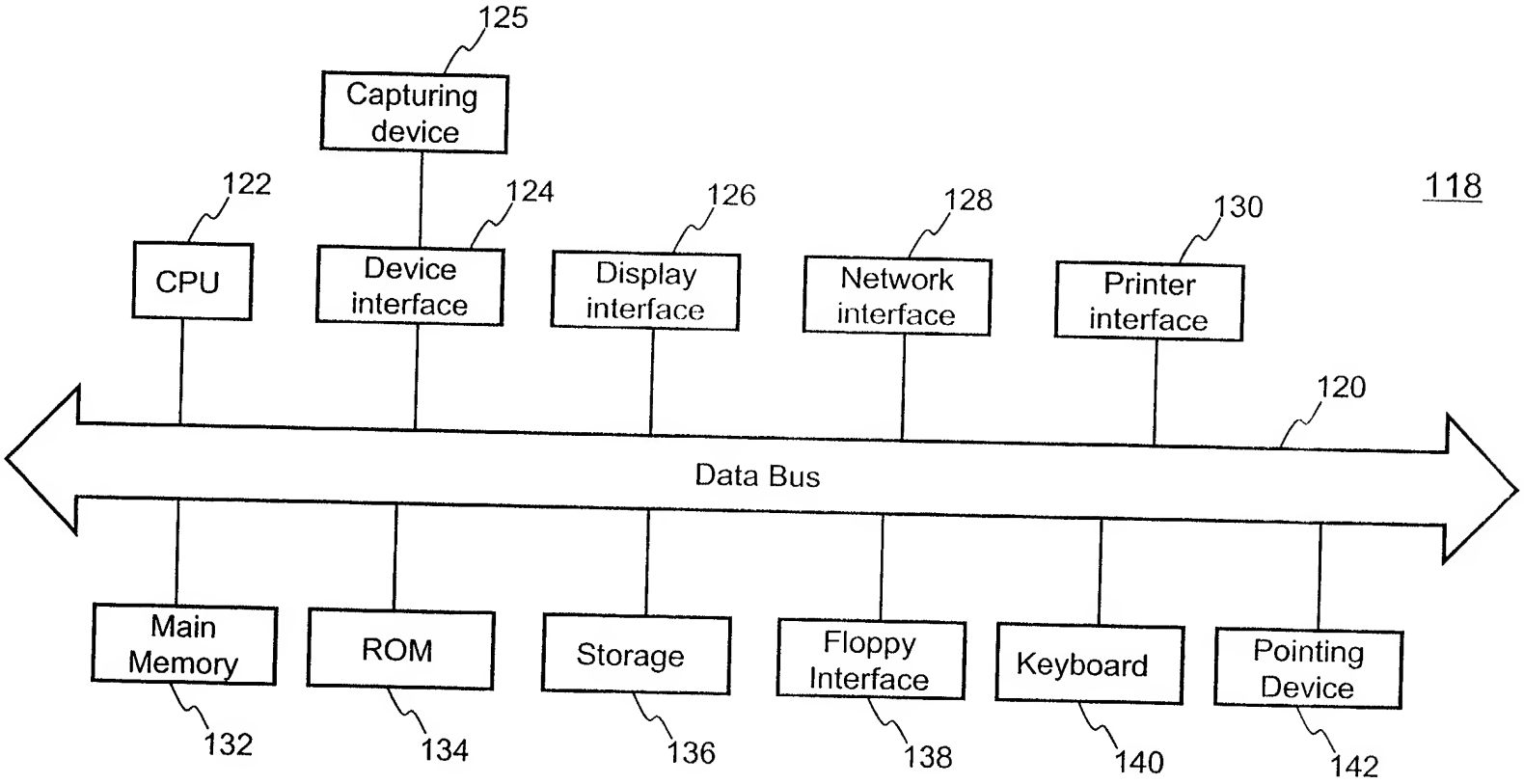

125
Capturing device
122
124
126
128
130
118
CPU
Device interface
Display interface
Network interface
Printer interface
120
Data Bus
Main Memory
ROM
Storage
Floppy Interface
Keyboard
Pointing Device
132
134
136
138
140
142

Fig. 1D

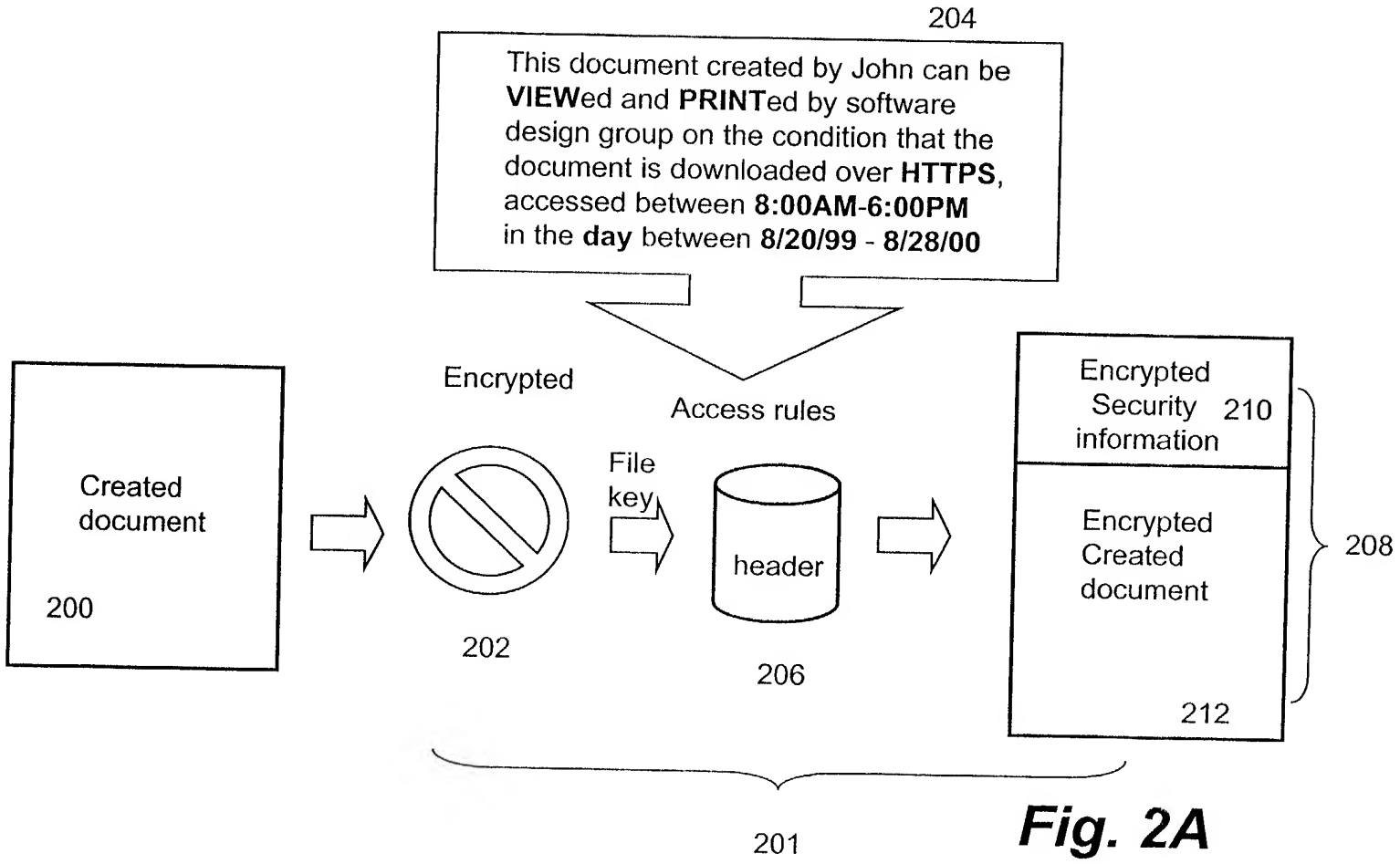

204
This document created by John can be **VIEW**ed and **PRINT**ed by software design group on the condition that the document is downloaded over **HTTPS**, accessed between **8:00AM-6:00PM** in the **day** between **8/20/99 - 8/28/00**
Encrypted
Access rules
Created document
200
File key
header
202
206
Encrypted Security information
210
Encrypted Created document
208
212
201

Fig. 2A

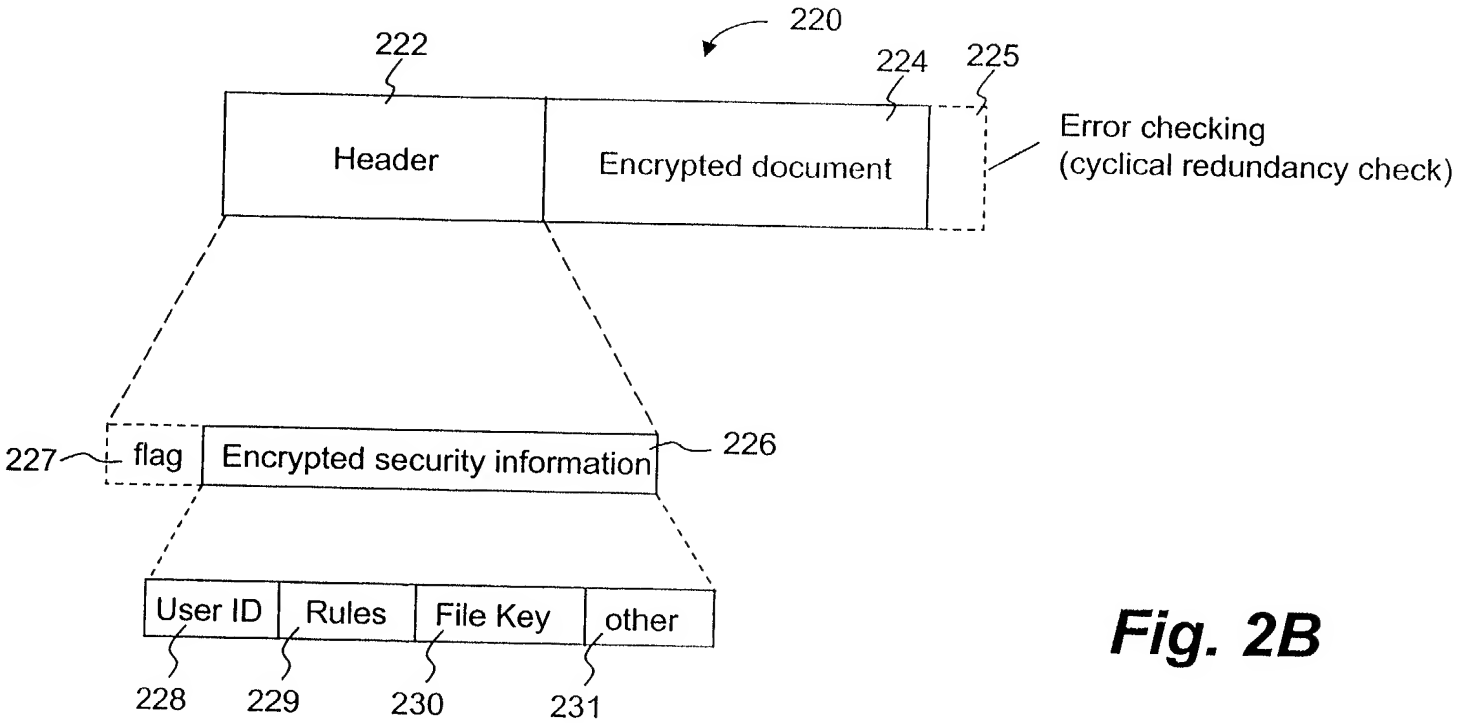

220
222
224
225
Header
Encrypted document
Error checking
(cyclical redundancy check)
227
flag
Encrypted security information
226
User ID
Rules
File Key
other
228
229
230
231

Fig. 2B

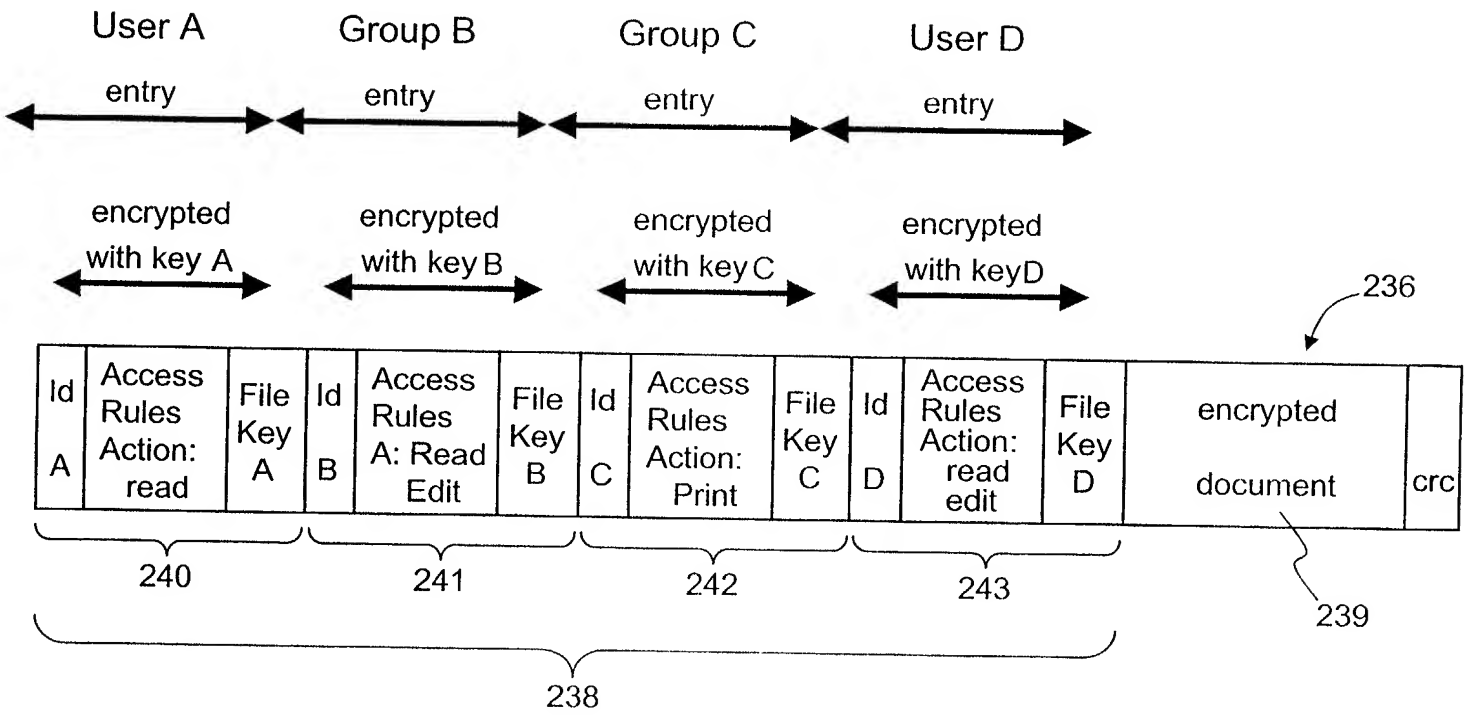

User A
Group B
Group C
User D
entry
entry
entry
entry
encrypted with key A
encrypted with key B
encrypted with key C
encrypted with keyD
236
Id A
Access Rules Action: read
File Key A
Id B
Access Rules A: Read Edit
File Key B
Id C
Access Rules Action: Print
File Key C
Id D
Access Rules Action: read edit
File Key D
encrypted document
crc
240
241
242
243
239
238

Fig. 2C.1

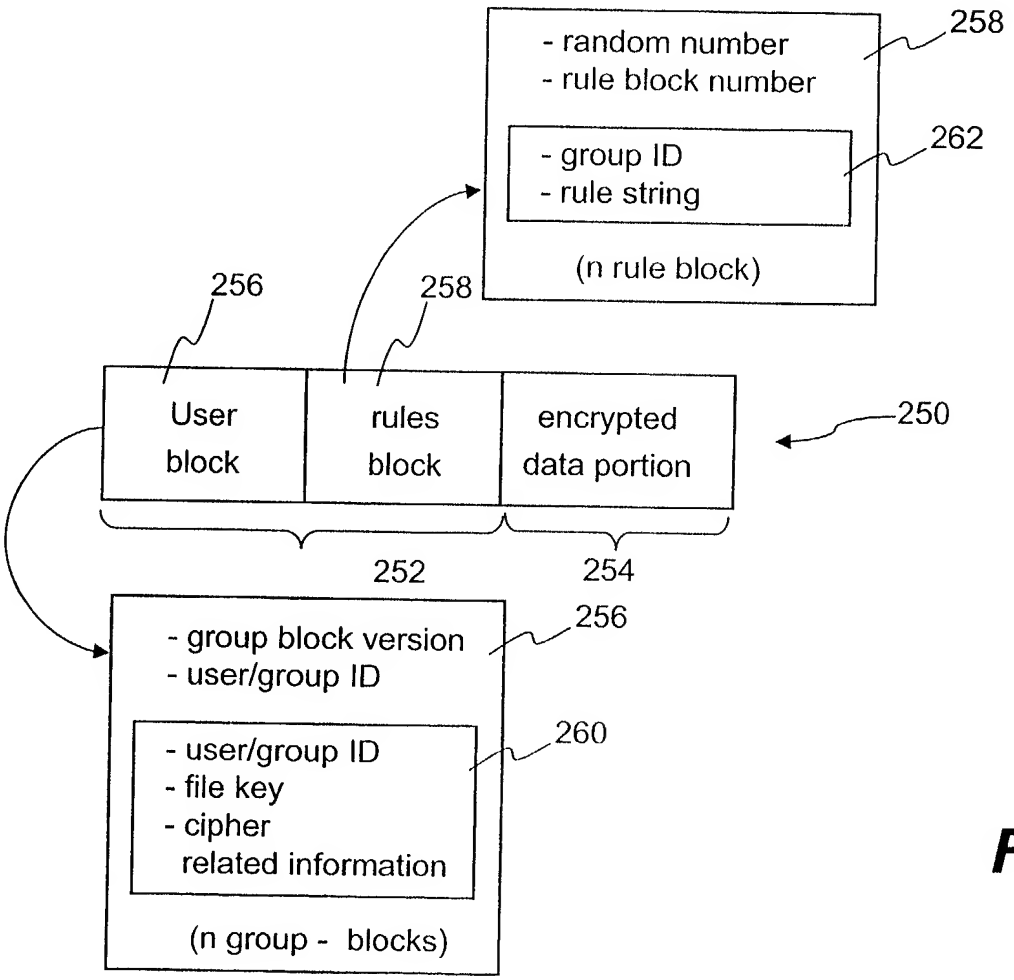

- random number
- rule block number
258
- group ID
- rule string
262
(n rule block)
256
258
User block
rules block
encrypted data portion
250
252
254
- group block version
- user/group ID
256
- user/group ID
- file key
- cipher related information
260
(n group - blocks)

Fig. 2C.2

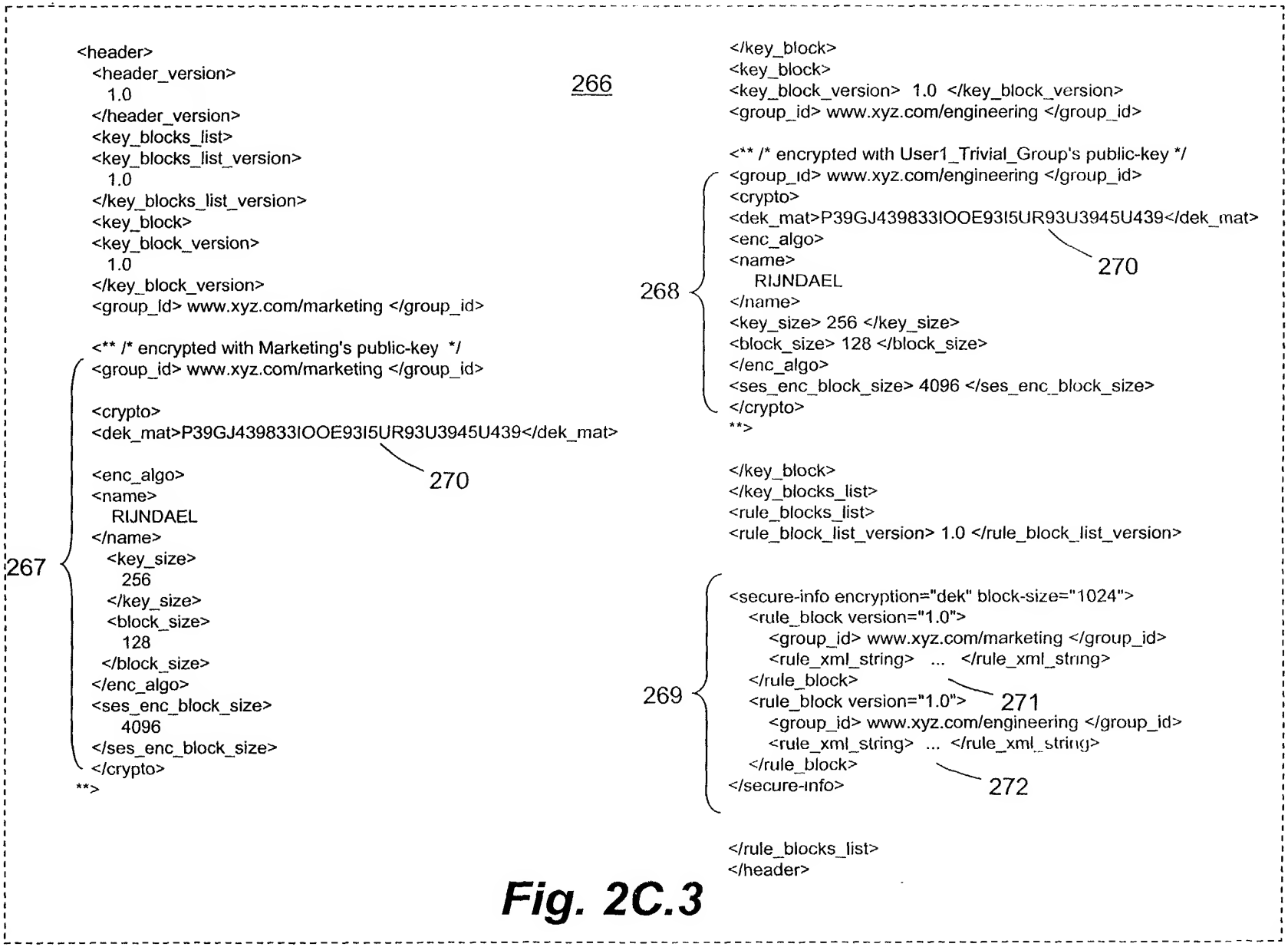

266
<header>
<header_version>
1.0
</header_version>
<key_blocks_list>
<key_blocks_list_version>
1.0
</key_blocks_list_version>
<key_block>
<key_block_version>
1.0
</key_block_version>
<group_id> www.xyz.com/marketing </group_id>
<** /* encrypted with Marketing's public-key */
<group_id> www.xyz.com/marketing </group_id>
<crypto>
<dek_mat>P39GJ439833IOOE93I5UR93U3945U439</dek_mat>
270
<enc_algo>
<name>
RIJNDAEL
</name>
<key_size>
256
</key_size>
<block_size>
128
</block_size>
</enc_algo>
<ses_enc_block_size>
4096
</ses_enc_block_size>
</crypto>
**>
267
</key_block>
<key_block>
<key_block_version> 1.0 </key_block_version>
<group_id> www.xyz.com/engineering </group_id>
<** /* encrypted with User1_Trivial_Group's public-key */
<group_id> www.xyz.com/engineering </group_id>
<crypto>
<dek_mat>P39GJ439833IOOE93I5UR93U3945U439</dek_mat>
270
<enc_algo>
<name>
RIJNDAEL
</name>
<key_size> 256 </key_size>
<block_size> 128 </block_size>
</enc_algo>
<ses_enc_block_size> 4096 </ses_enc_block_size>
</crypto>
**>
268
</key_block>
</key_blocks_list>
<rule_blocks_list>
<rule_block_list_version> 1.0 </rule_block_list_version>
<secure-info encryption="dek" block-size="1024">
<rule_block version="1.0">
<group_id> www.xyz.com/marketing </group_id>
<rule_xml_string> ... </rule_xml_string>
</rule_block>
<rule_block version="1.0">
271
<group_id> www.xyz.com/engineering </group_id>
<rule_xml_string> ... </rule_xml_string>
</rule_block>
</secure-info>
272
269
</rule_blocks_list>
</header>

Fig. 2C.3

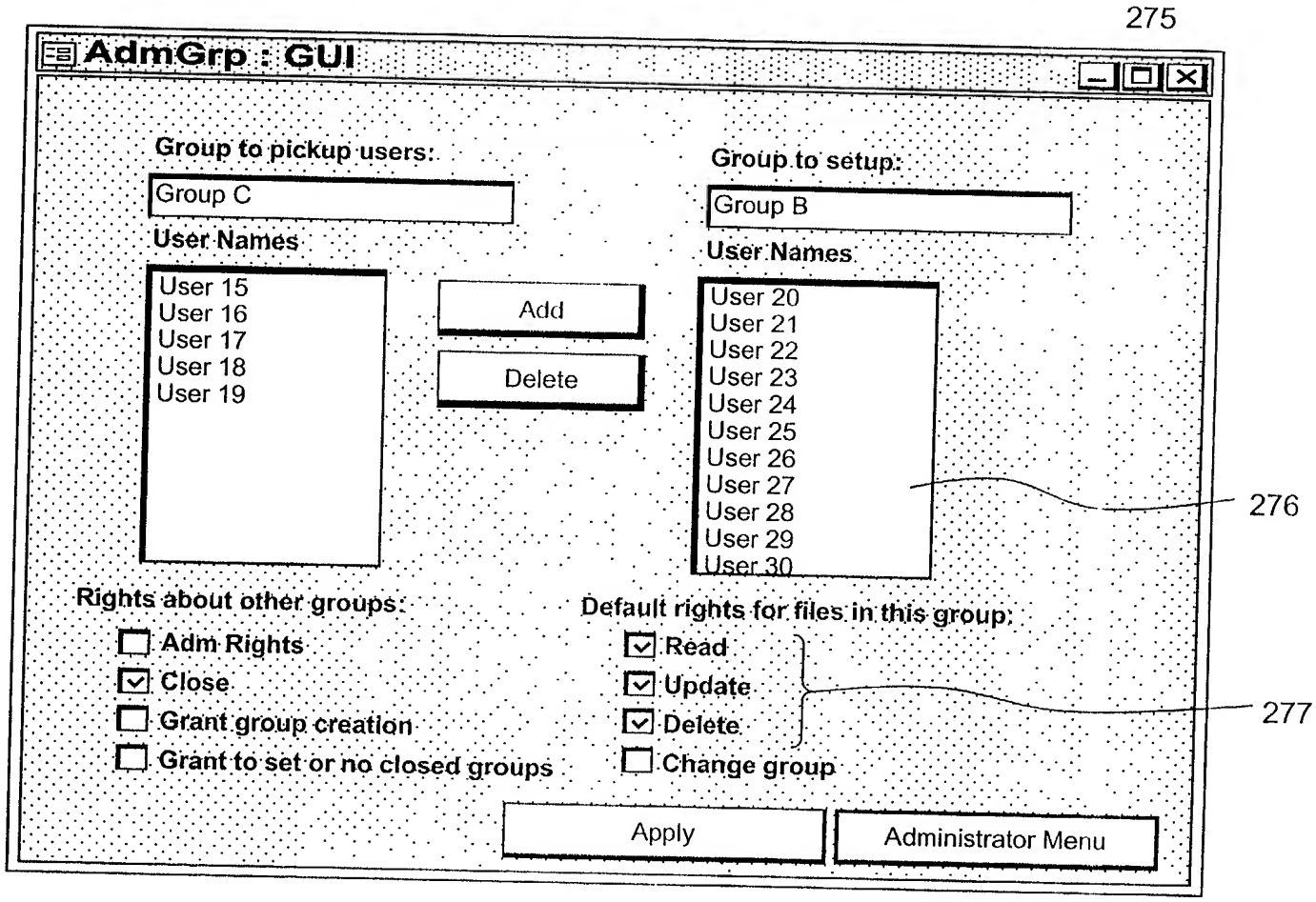

275
AdmGrp : GUI
Group to pickup users:
Group C
User Names
User 15
User 16
User 17
User 18
User 19
Add
Delete
Group to setup:
Group B
User Names
User 20
User 21
User 22
User 23
User 24
User 25
User 26
User 27
User 28
User 29
User 30
276
Rights about other groups:
Adm Rights
Close
Grant group creation
Grant to set or no closed groups
Default rights for files in this group:
Read
Update
Delete
Change group
277
Apply
Administrator Menu

Fig. 2D

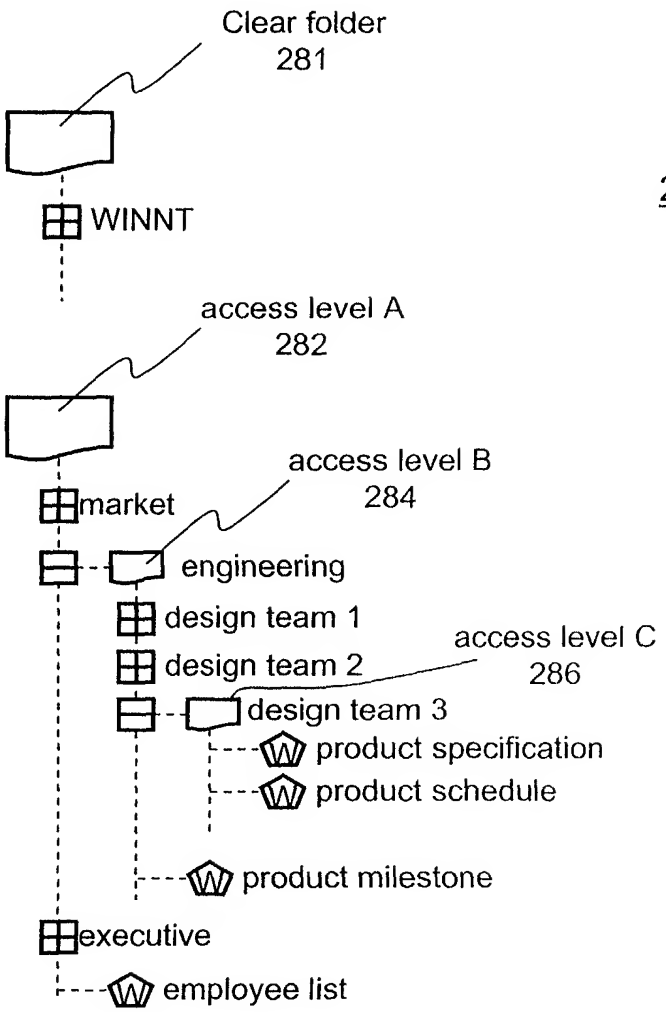

Clear folder
281
280
WINNT
access level A
282
access level B
284
market
engineering
design team 1
design team 2
access level C
286
design team 3
product specification
product schedule
product milestone
executive
employee list

Fig. 2E

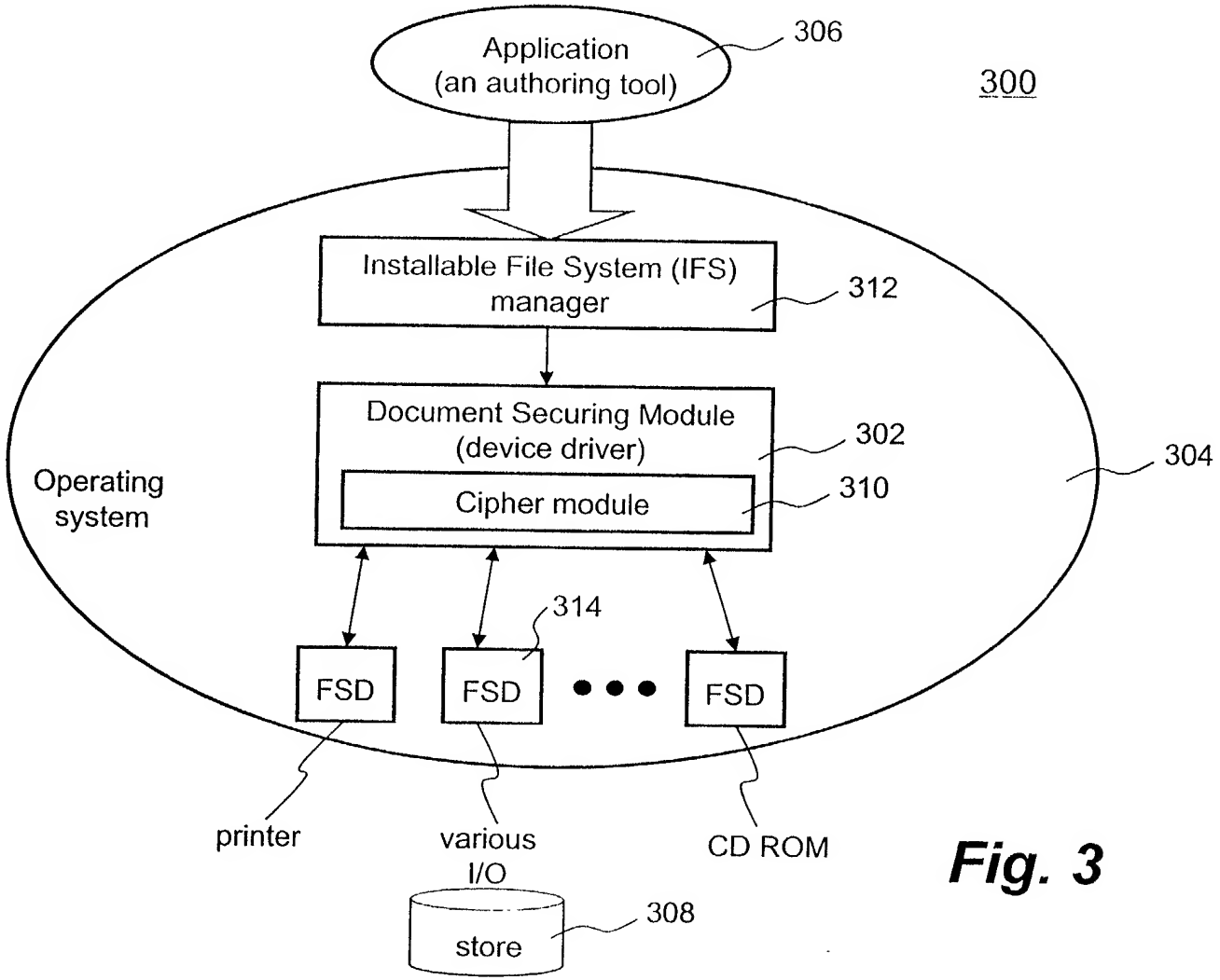

Application
(an authoring tool)
306
300
Installable File System (IFS)
manager
312
Document Securing Module
(device driver)
302
Cipher module
310
Operating
system
304
314
FSD
FSD
FSD
printer
various
I/O
CD ROM
store
308

Fig. 3

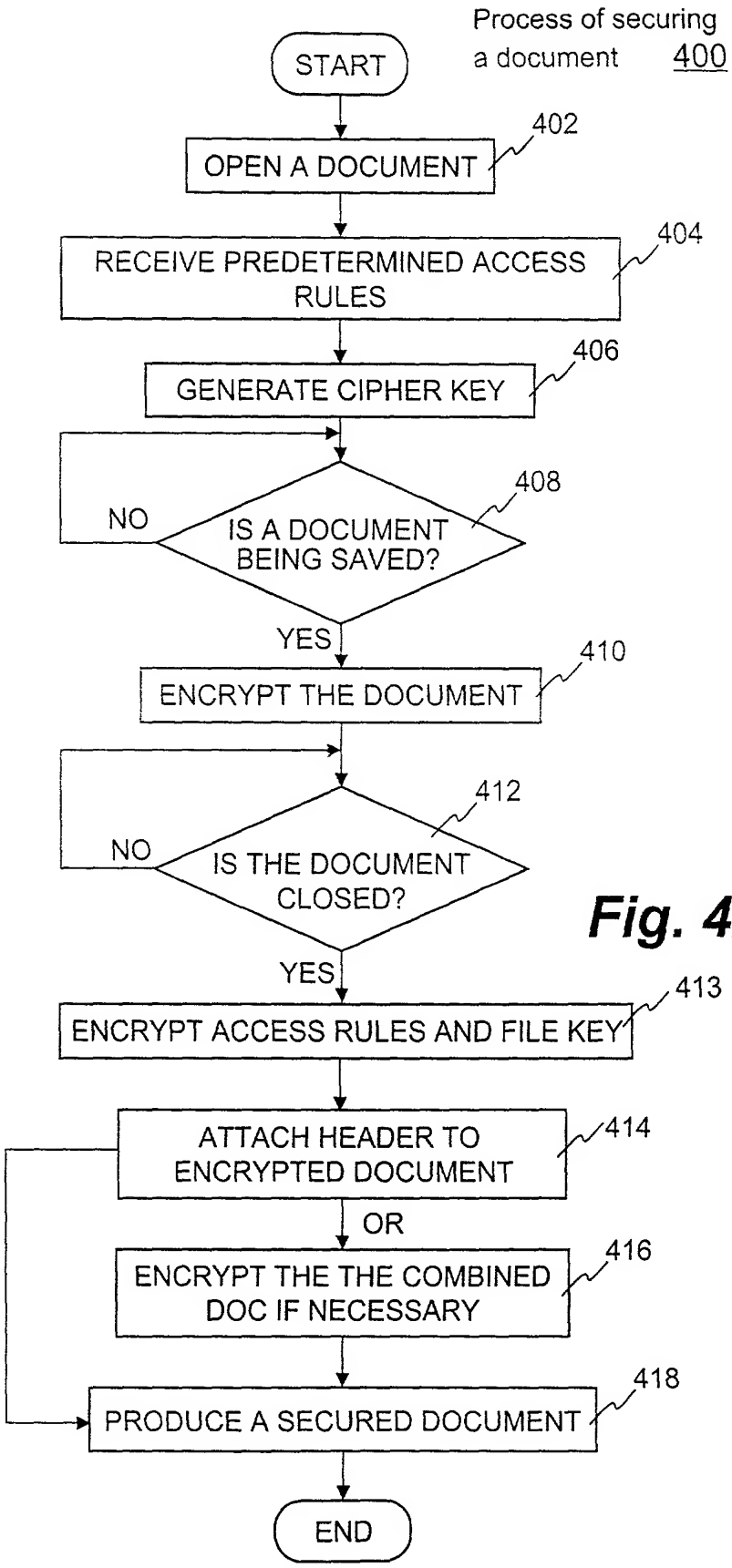

Process of securing a document 400
START
402
OPEN A DOCUMENT
404
RECEIVE PREDETERMINED ACCESS RULES
406
GENERATE CIPHER KEY
408
NO
IS A DOCUMENT BEING SAVED?
YES
410
ENCRYPT THE DOCUMENT
412
NO
IS THE DOCUMENT CLOSED?
YES
413
ENCRYPT ACCESS RULES AND FILE KEY
414
ATTACH HEADER TO ENCRYPTED DOCUMENT
OR
416
ENCRYPT THE THE COMBINED DOC IF NECESSARY
418
PRODUCE A SECURED DOCUMENT
END

Fig. 4A

Process of receiving access rules 430

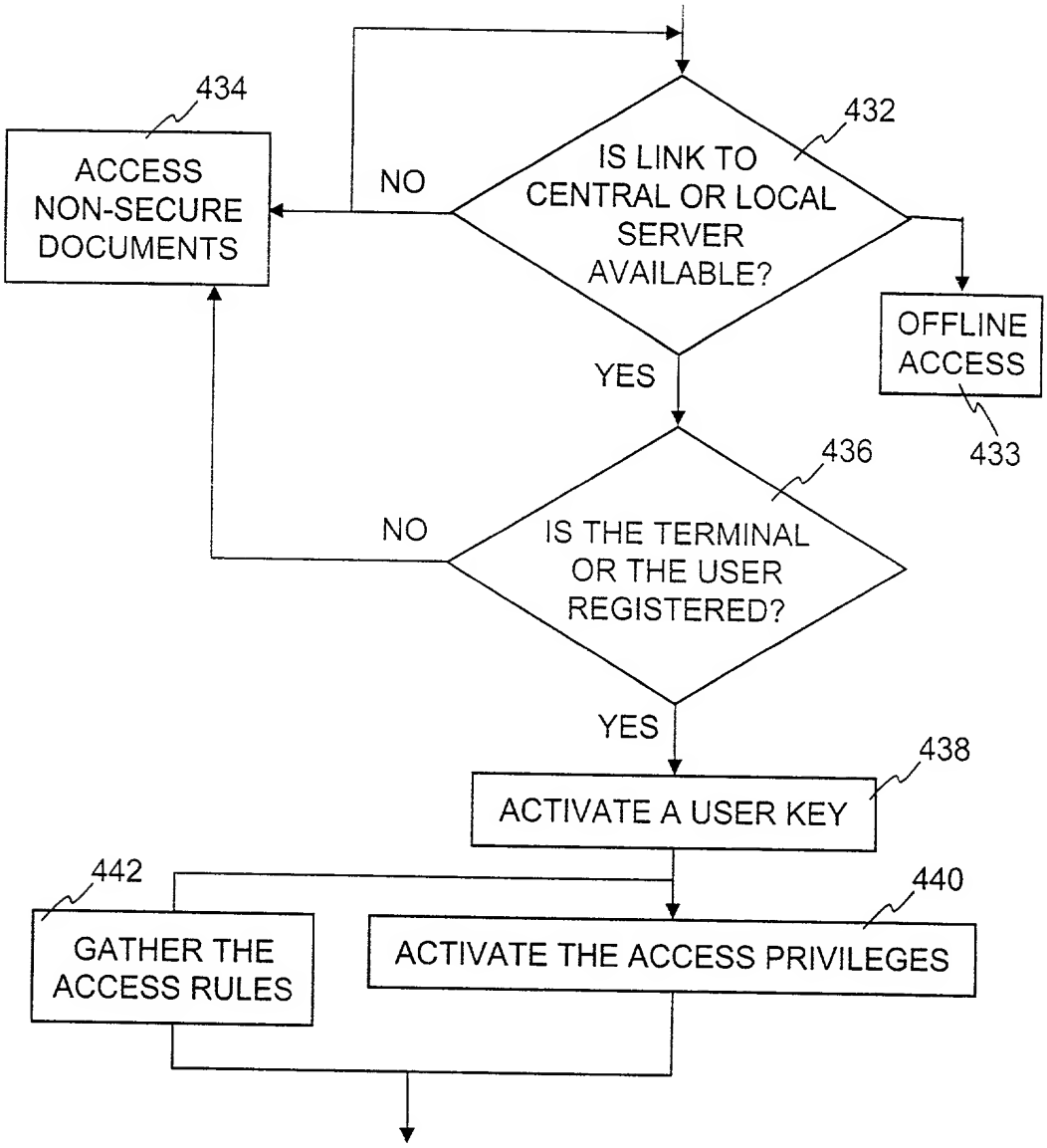
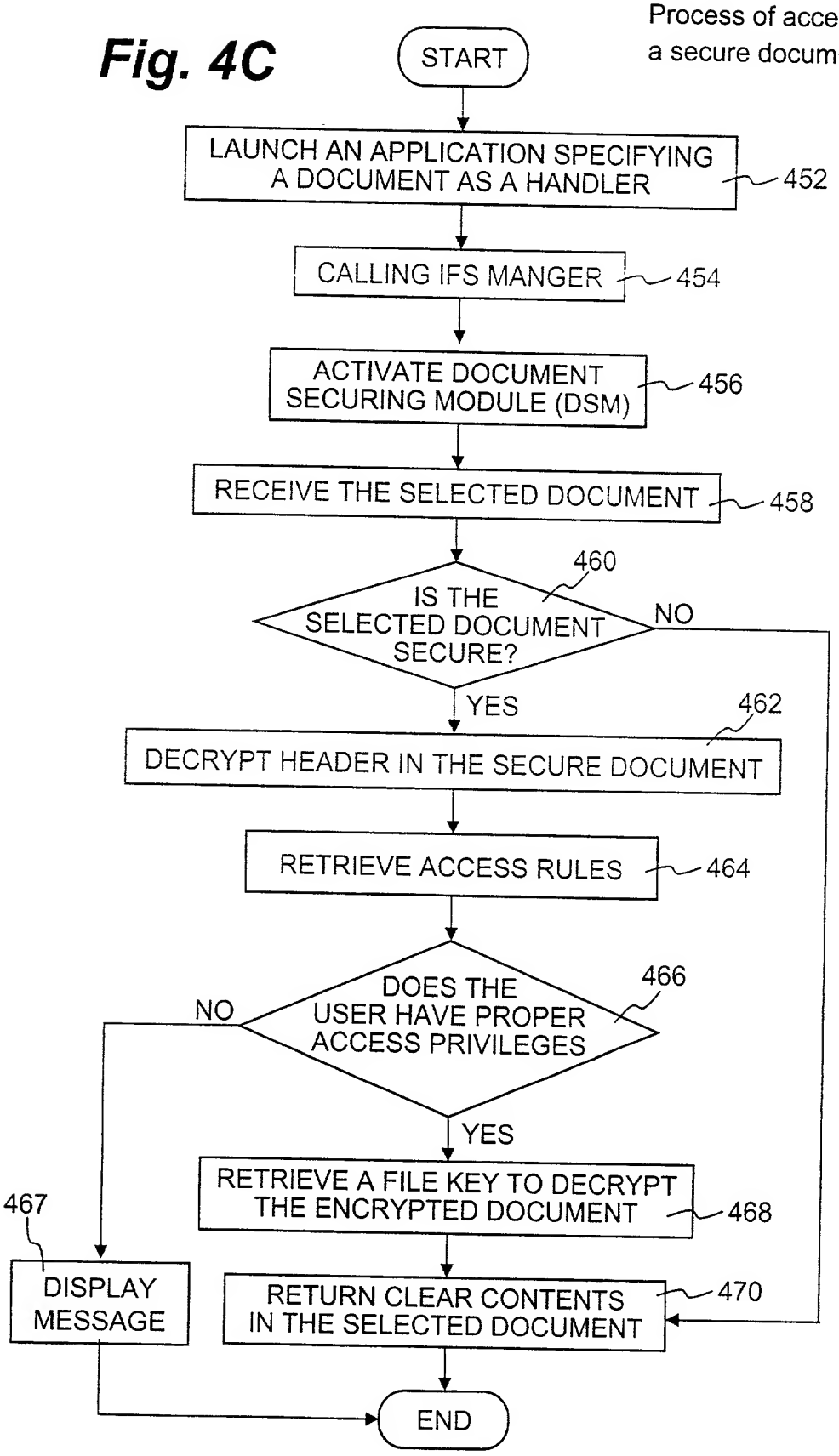


Fig. 4B

Fig. 4C


Process of accessing a secure document 450
START
LAUNCH AN APPLICATION SPECIFYING A DOCUMENT AS A HANDLER
452
CALLING IFS MANGER
454
ACTIVATE DOCUMENT SECURING MODULE (DSM)
456
RECEIVE THE SELECTED DOCUMENT
458
460
IS THE SELECTED DOCUMENT SECURE?
NO
YES
462
DECRYPT HEADER IN THE SECURE DOCUMENT
RETRIEVE ACCESS RULES
464
DOES THE USER HAVE PROPER ACCESS PRIVILEGES
466
NO
YES
RETRIEVE A FILE KEY TO DECRYPT THE ENCRYPTED DOCUMENT
468
467
DISPLAY MESSAGE
RETURN CLEAR CONTENTS IN THE SELECTED DOCUMENT
470
END

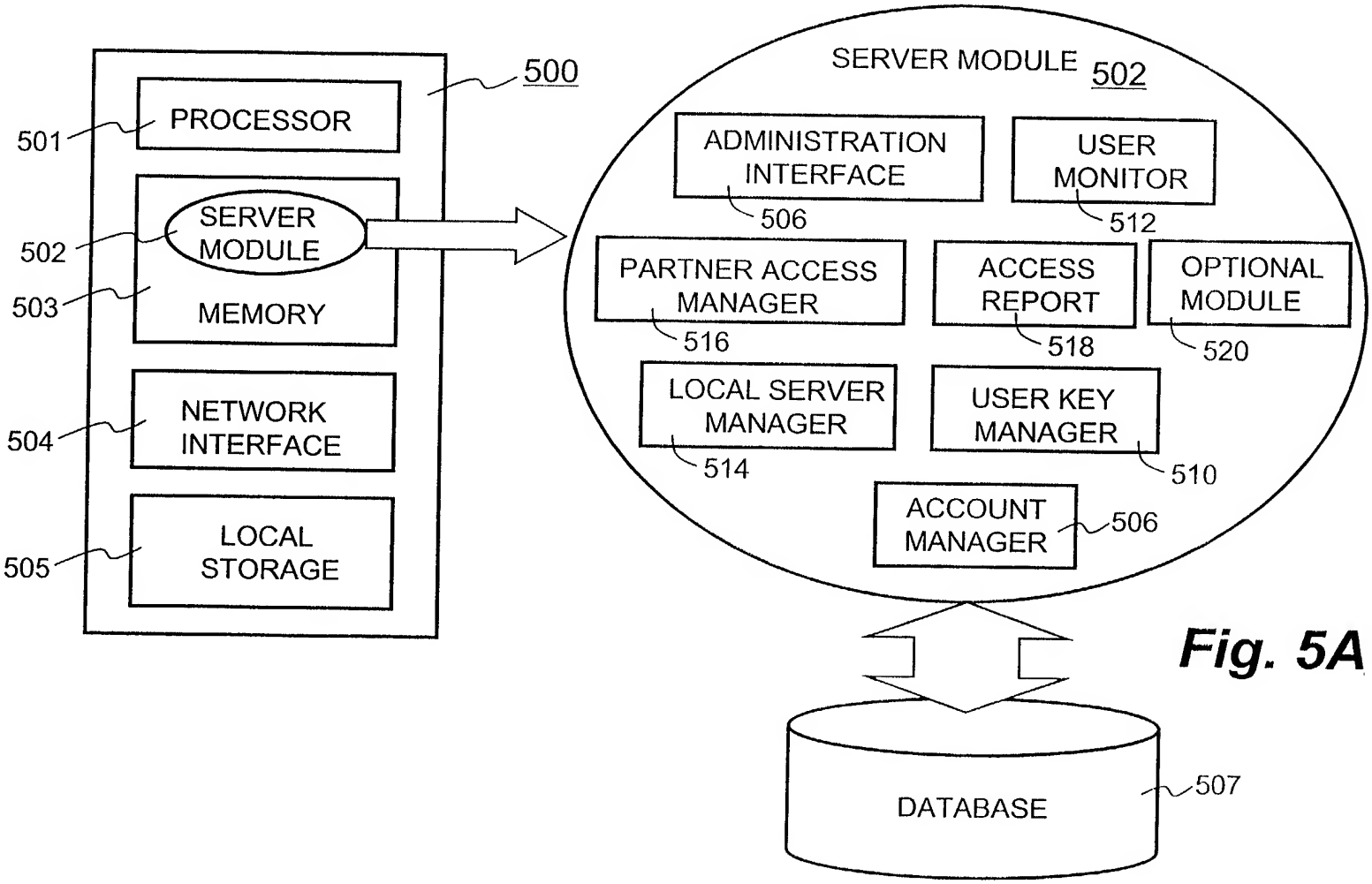

500
PROCESSOR
501
SERVER MODULE
502
MEMORY
503
NETWORK INTERFACE
504
LOCAL STORAGE
505
SERVER MODULE 502
ADMINISTRATION INTERFACE
506
USER MONITOR
512
PARTNER ACCESS MANAGER
516
ACCESS REPORT
518
OPTIONAL MODULE
520
LOCAL SERVER MANAGER
514
USER KEY MANAGER
510
ACCOUNT MANAGER
506
DATABASE
507

Fig. 5A

User ID	User	Open	Edit	Write	Print	Copy	Download	Others
01243	User A	Y	Y	Y	Y	Y	Y	Y
17364	User B	Y			Y			
18465	G User C	Y	Y	Y			Y	
• • •								

Fig. 5B.1

All user keys	Key/Key pair	Location	others
John's	111101101010101	128.1.100.64, ...	
Mike's, Dell's	101011000111111	64.100.1.128, ...	
Finance group	010101010111111	64.100.1.100, ...	
• • •			

Fig. 5B.2

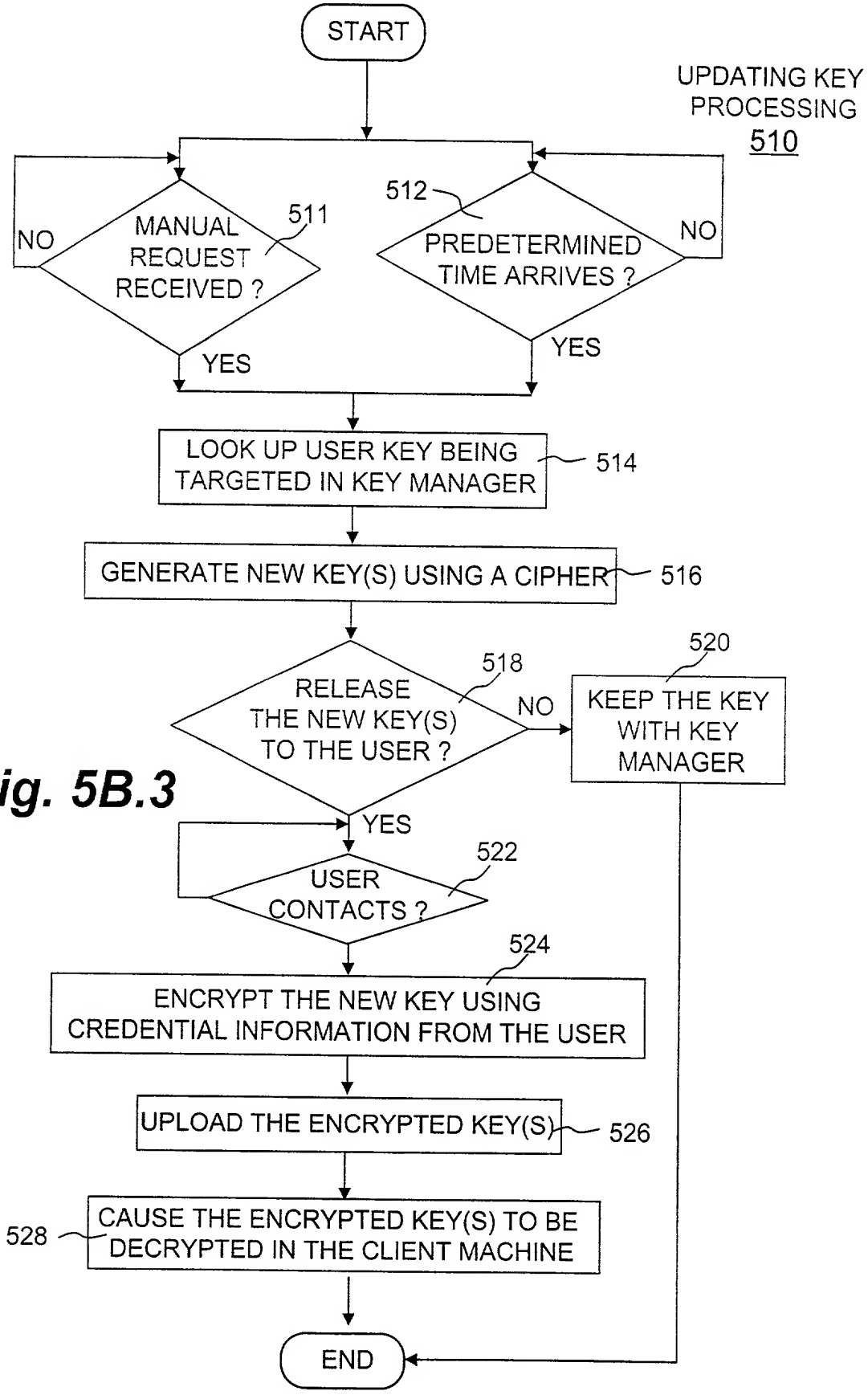

START
UPDATING KEY PROCESSING
510
MANUAL REQUEST RECEIVED ?
511
NO
YES
PREDETERMINED TIME ARRIVES ?
512
NO
YES
LOOK UP USER KEY BEING TARGETED IN KEY MANAGER
514
GENERATE NEW KEY(S) USING A CIPHER
516
RELEASE THE NEW KEY(S) TO THE USER ?
518
NO
KEEP THE KEY WITH KEY MANAGER
520
YES
USER CONTACTS ?
522
ENCRYPT THE NEW KEY USING CREDENTIAL INFORMATION FROM THE USER
524
UPLOAD THE ENCRYPTED KEY(S)
526
CAUSE THE ENCRYPTED KEY(S) TO BE DECRYPTED IN THE CLIENT MACHINE
528
END

Fig. 5B.3

Server Assisted Process of Accessing secure document 530

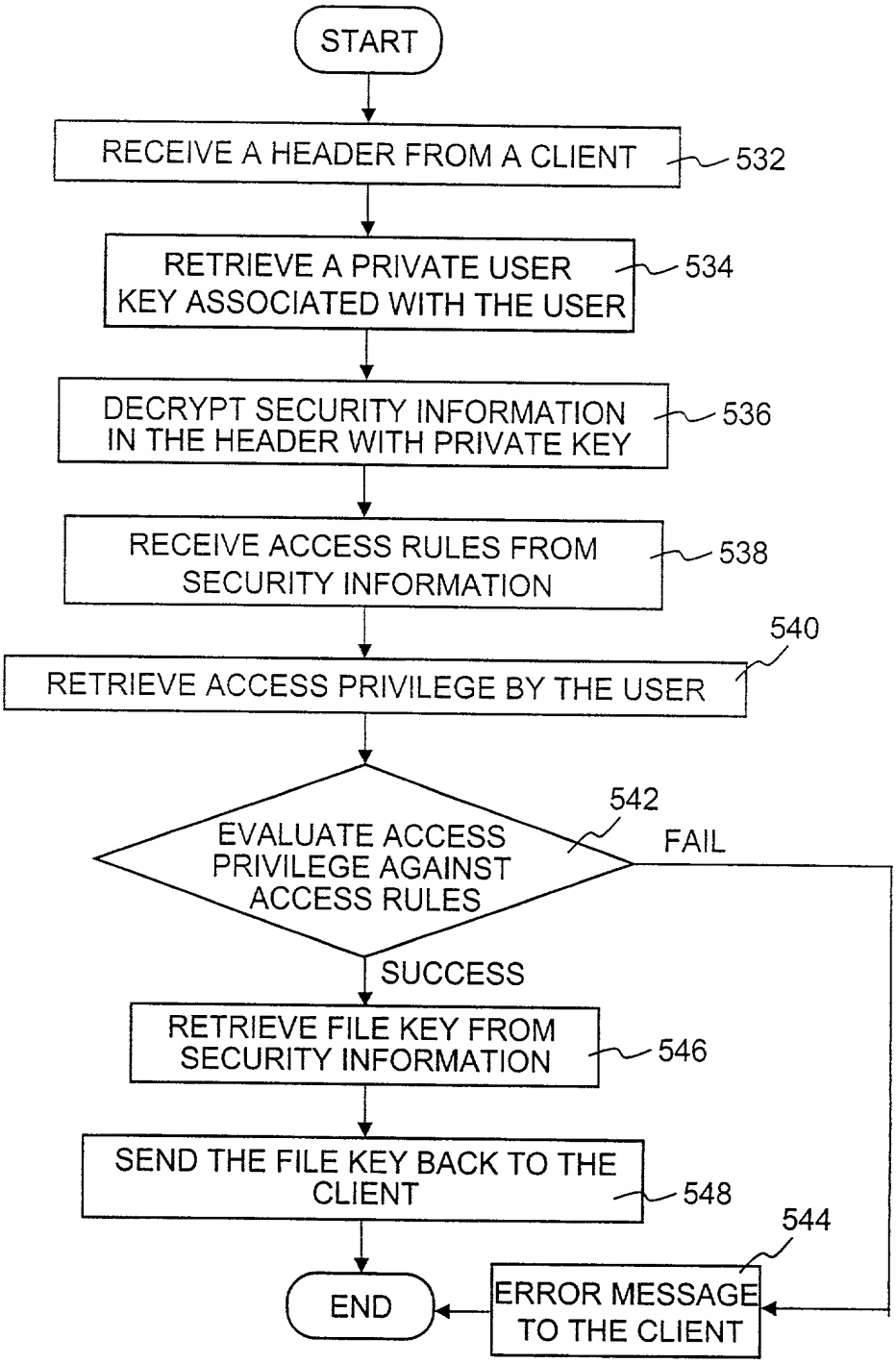


Fig. 5B.4

Server Assisted Process
of securing a document
550

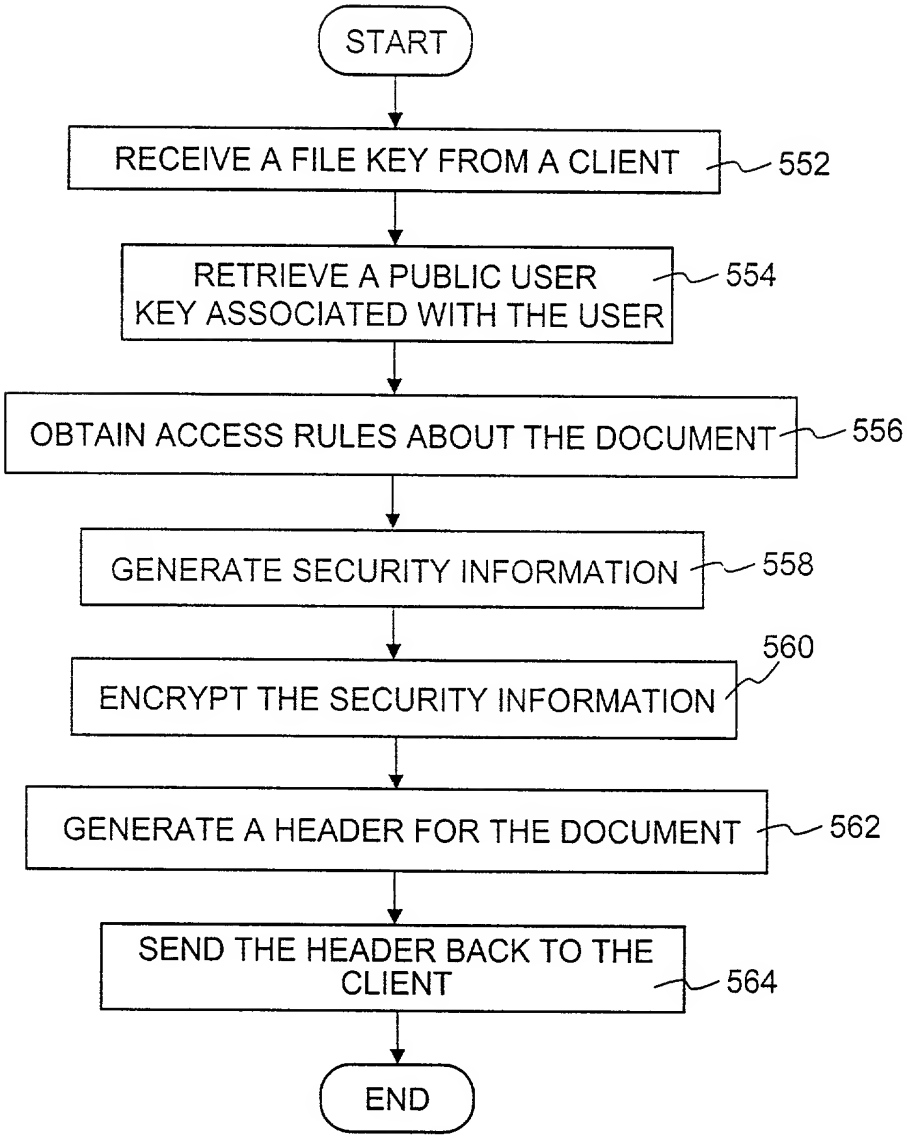


Fig. 5B.5

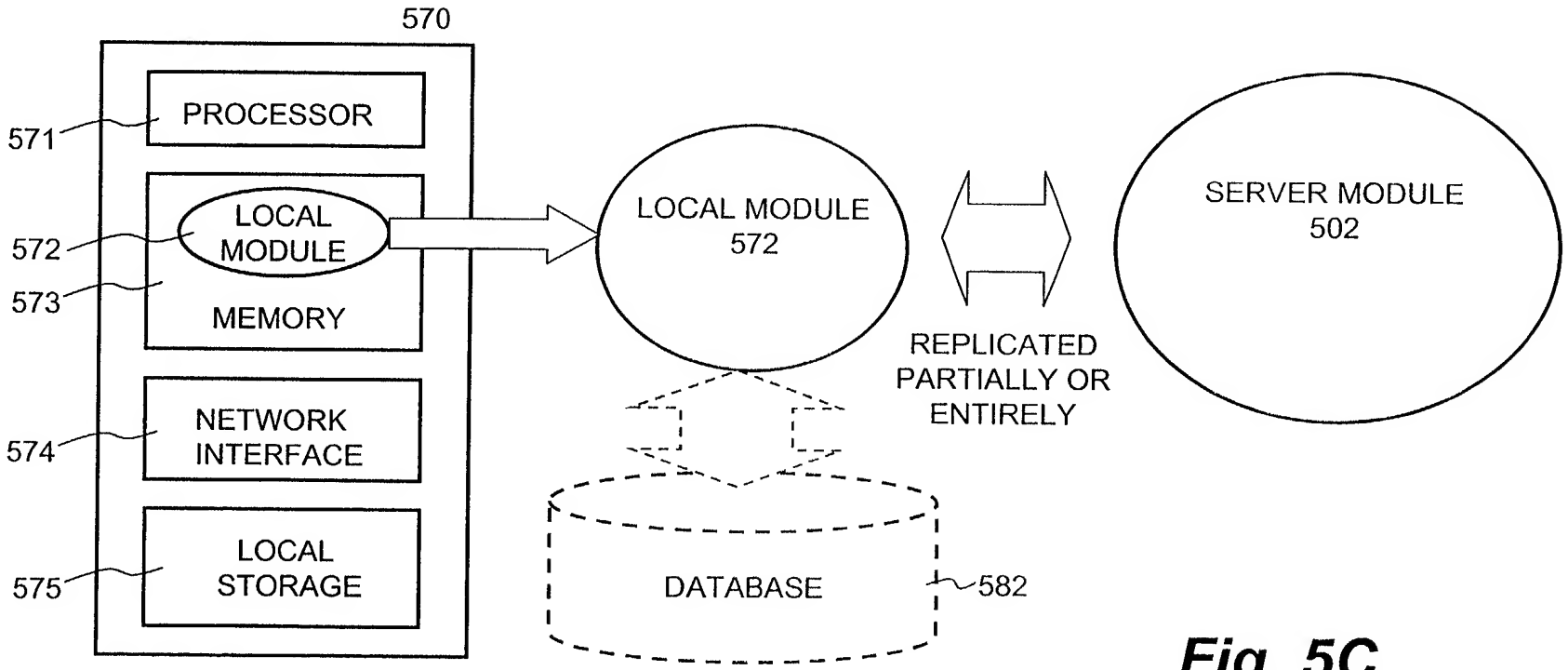

570
PROCESSOR
571
LOCAL MODULE
572
572
573
MEMORY
NETWORK INTERFACE
574
LOCAL STORAGE
575
LOCAL MODULE 572
REPLICATED PARTIALLY OR ENTIRELY
SERVER MODULE 502
DATABASE
582

Fig. 5C

584

USER	PASSWORD	ACCESS PRIVILEGES	
John	*********	L=10, T=24, D=ALL, C=ALL	585
Dell	*********	L=1, T=8, D=M-F, C=A	586
Mike	*********	L=5, T=12, D=M-S, C=A & B	587
	⋮		

Fig. 5D

For Local Server A

USER	PASSWORD
John	*********
Dell	*********
Mike	*********
	⋮

For Local Server B

USER	PASSWORD
John	*********
Mike	*********
	⋮

For Local Server C

USER	PASSWORD
John	*********
	⋮

Fig. 5E

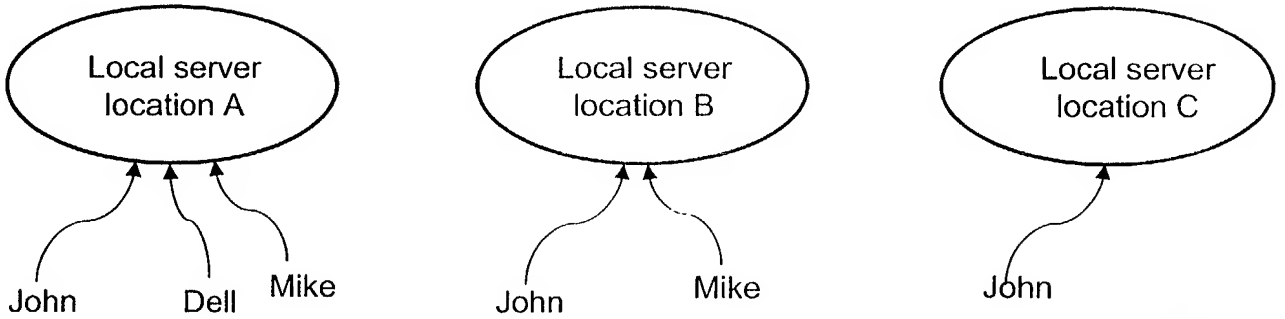

Local server location A
John
Dell
Mike
Local server location B
John
Mike
Local server location C
John

Fig. 5F

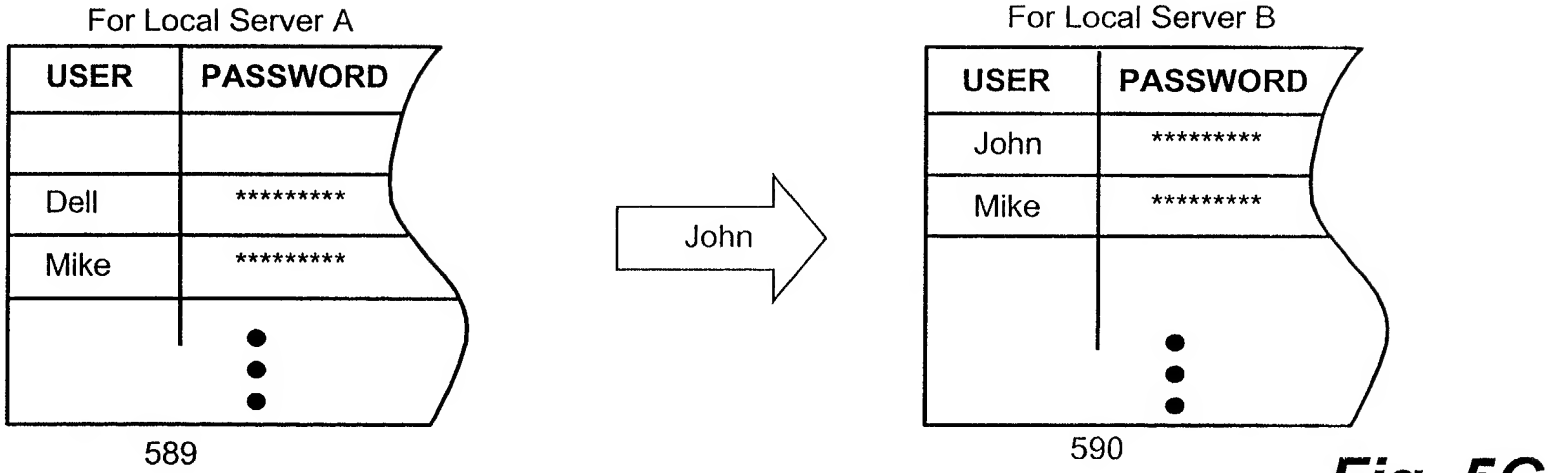

For Local Server A
USER
PASSWORD
Dell
****
Mike
****
589
John
For Local Server B
USER
PASSWORD
John
****
Mike
****
590

Fig. 5G

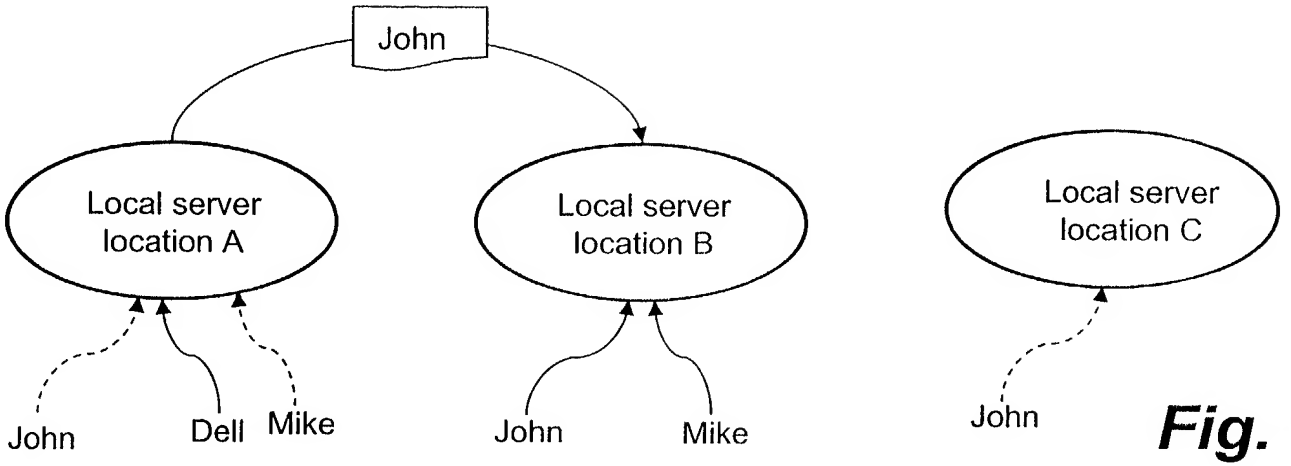

John
Local server location A
Local server location B
Local server location C
John
Dell
Mike
John
Mike
John

Fig. 5H

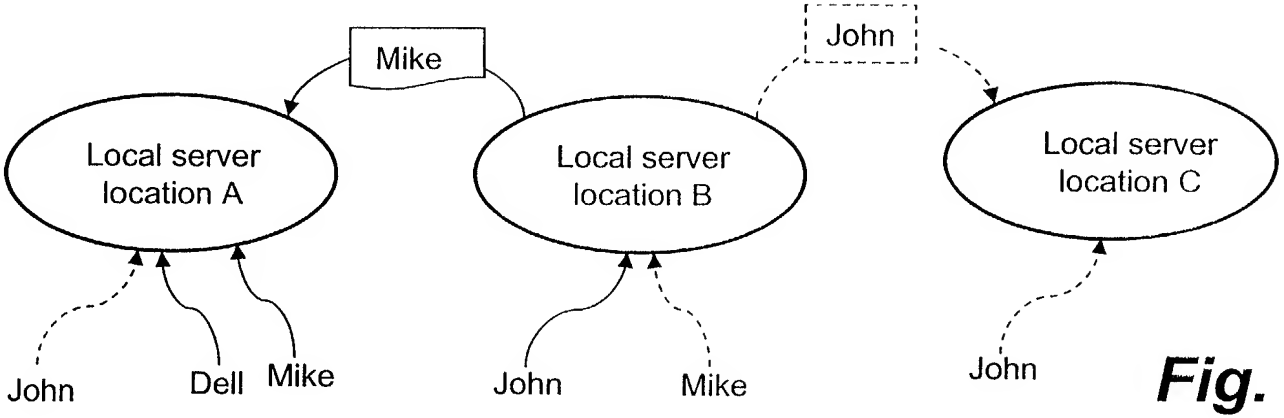

Mike
John
Local server location A
Local server location B
Local server location C
John
Dell
Mike
John
Mike
John

Fig. 5I

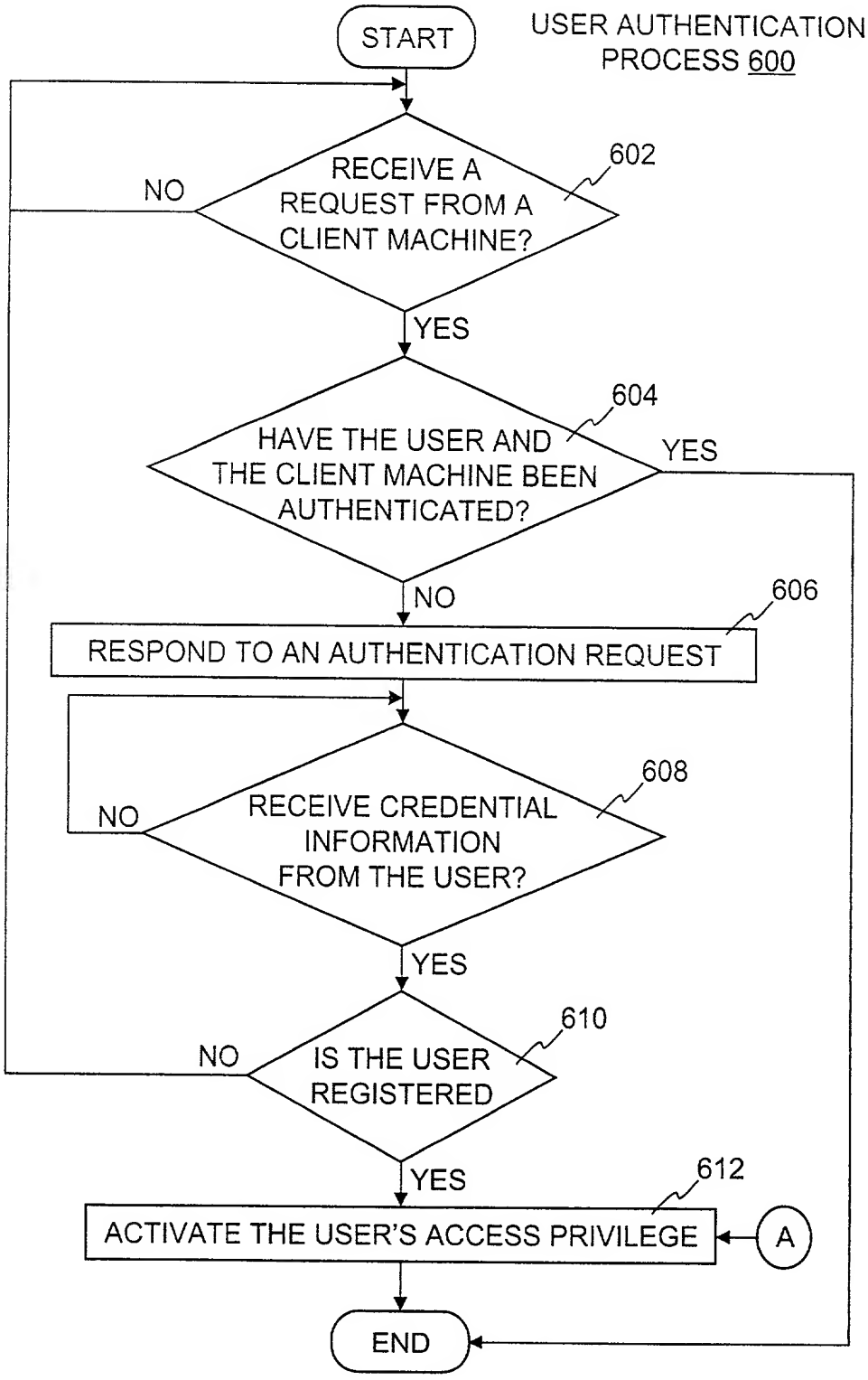

START
USER AUTHENTICATION PROCESS 600
602
RECEIVE A REQUEST FROM A CLIENT MACHINE?
NO
YES
604
HAVE THE USER AND THE CLIENT MACHINE BEEN AUTHENTICATED?
YES
NO
606
RESPOND TO AN AUTHENTICATION REQUEST
608
RECEIVE CREDENTIAL INFORMATION FROM THE USER?
NO
YES
610
IS THE USER REGISTERED
NO
YES
612
ACTIVATE THE USER'S ACCESS PRIVILEGE
A
END

Fig. 6A

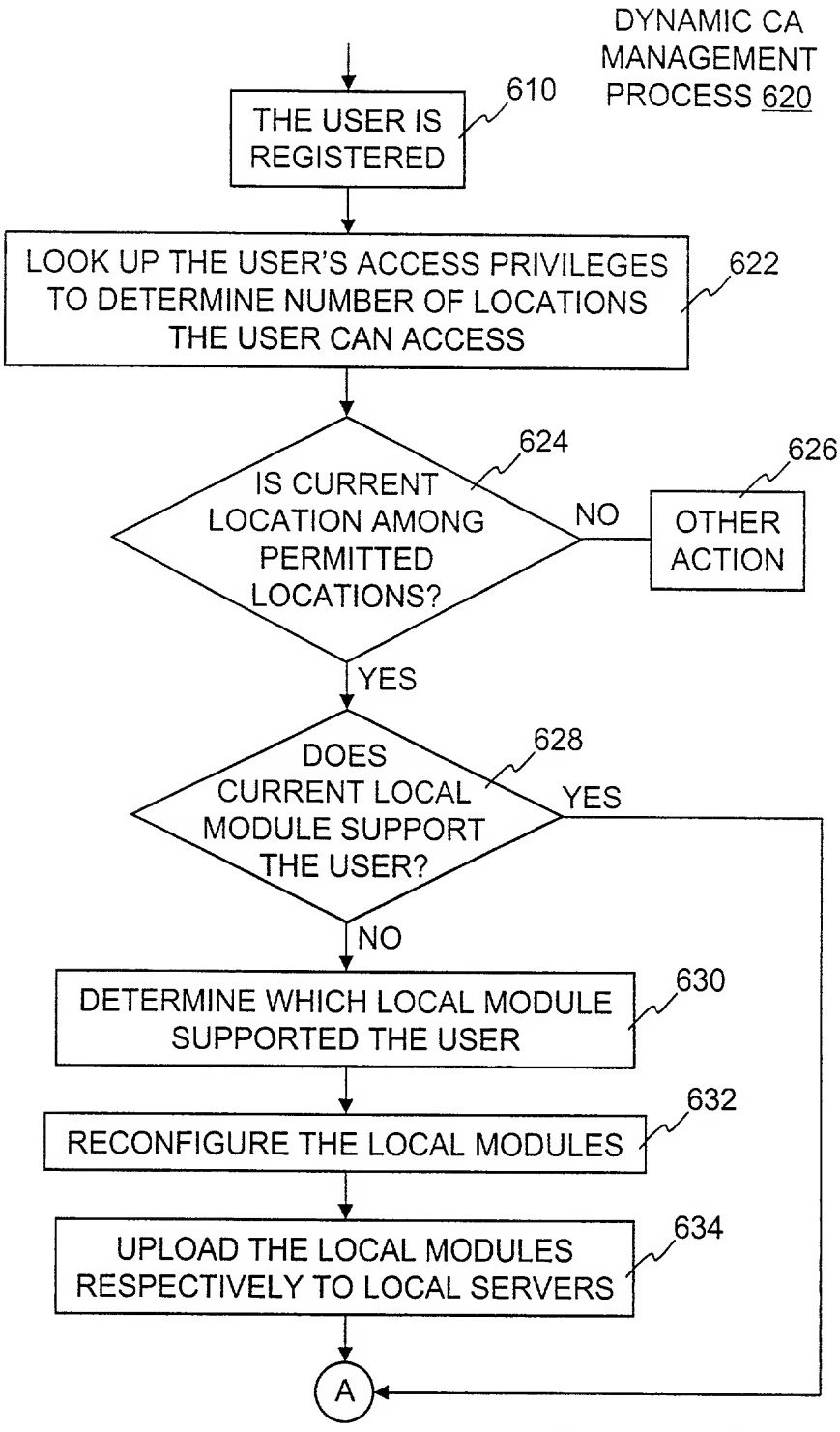

DYNAMIC CA MANAGEMENT PROCESS 620
610
THE USER IS REGISTERED
LOOK UP THE USER'S ACCESS PRIVILEGES TO DETERMINE NUMBER OF LOCATIONS THE USER CAN ACCESS
622
624
IS CURRENT LOCATION AMONG PERMITTED LOCATIONS?
NO
626
OTHER ACTION
YES
628
DOES CURRENT LOCAL MODULE SUPPORT THE USER?
YES
NO
630
DETERMINE WHICH LOCAL MODULE SUPPORTED THE USER
632
RECONFIGURE THE LOCAL MODULES
634
UPLOAD THE LOCAL MODULES RESPECTIVELY TO LOCAL SERVERS
A

Fig. 6B

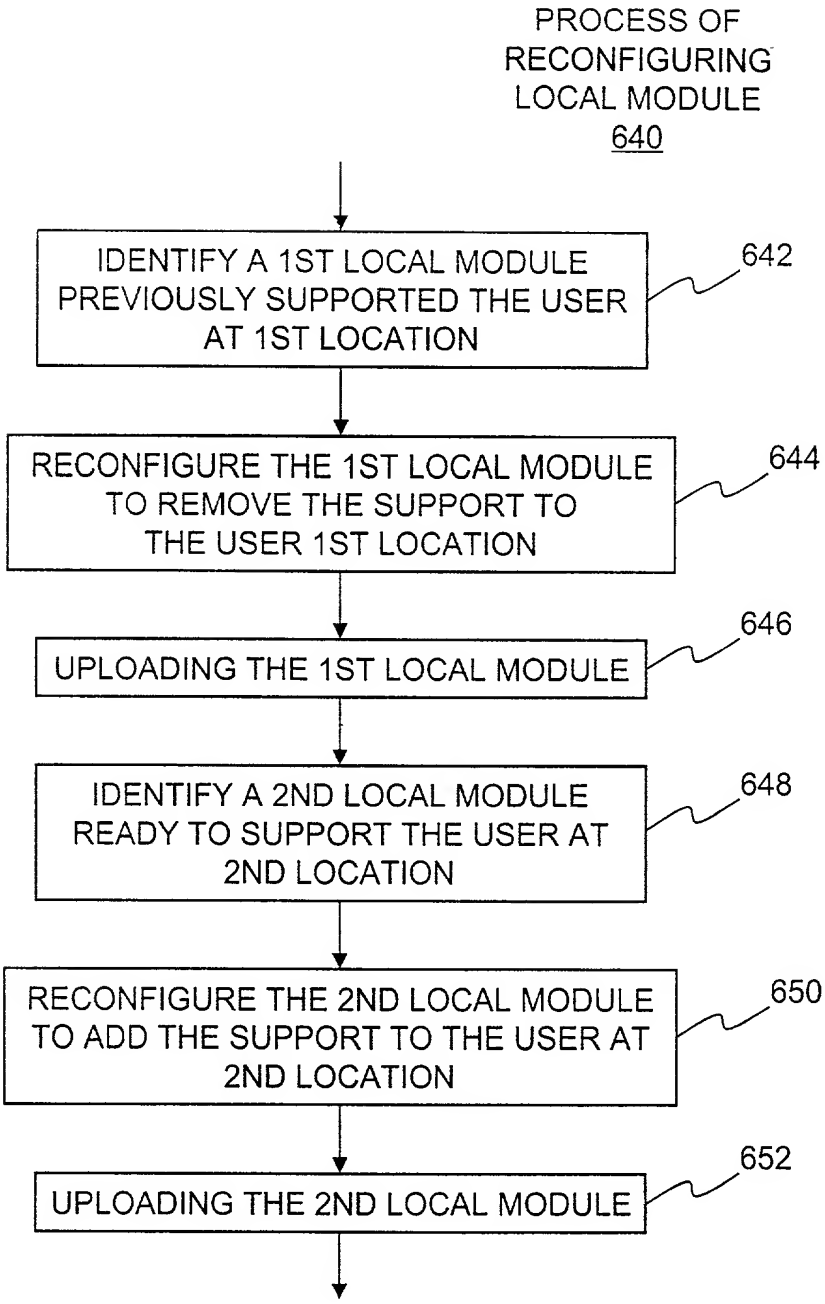

PROCESS OF RECONFIGURING LOCAL MODULE 640
IDENTIFY A 1ST LOCAL MODULE PREVIOUSLY SUPPORTED THE USER AT 1ST LOCATION
642
RECONFIGURE THE 1ST LOCAL MODULE TO REMOVE THE SUPPORT TO THE USER 1ST LOCATION
644
UPLOADING THE 1ST LOCAL MODULE
646
IDENTIFY A 2ND LOCAL MODULE READY TO SUPPORT THE USER AT 2ND LOCATION
648
RECONFIGURE THE 2ND LOCAL MODULE TO ADD THE SUPPORT TO THE USER AT 2ND LOCATION
650
UPLOADING THE 2ND LOCAL MODULE
652

Fig. 6C

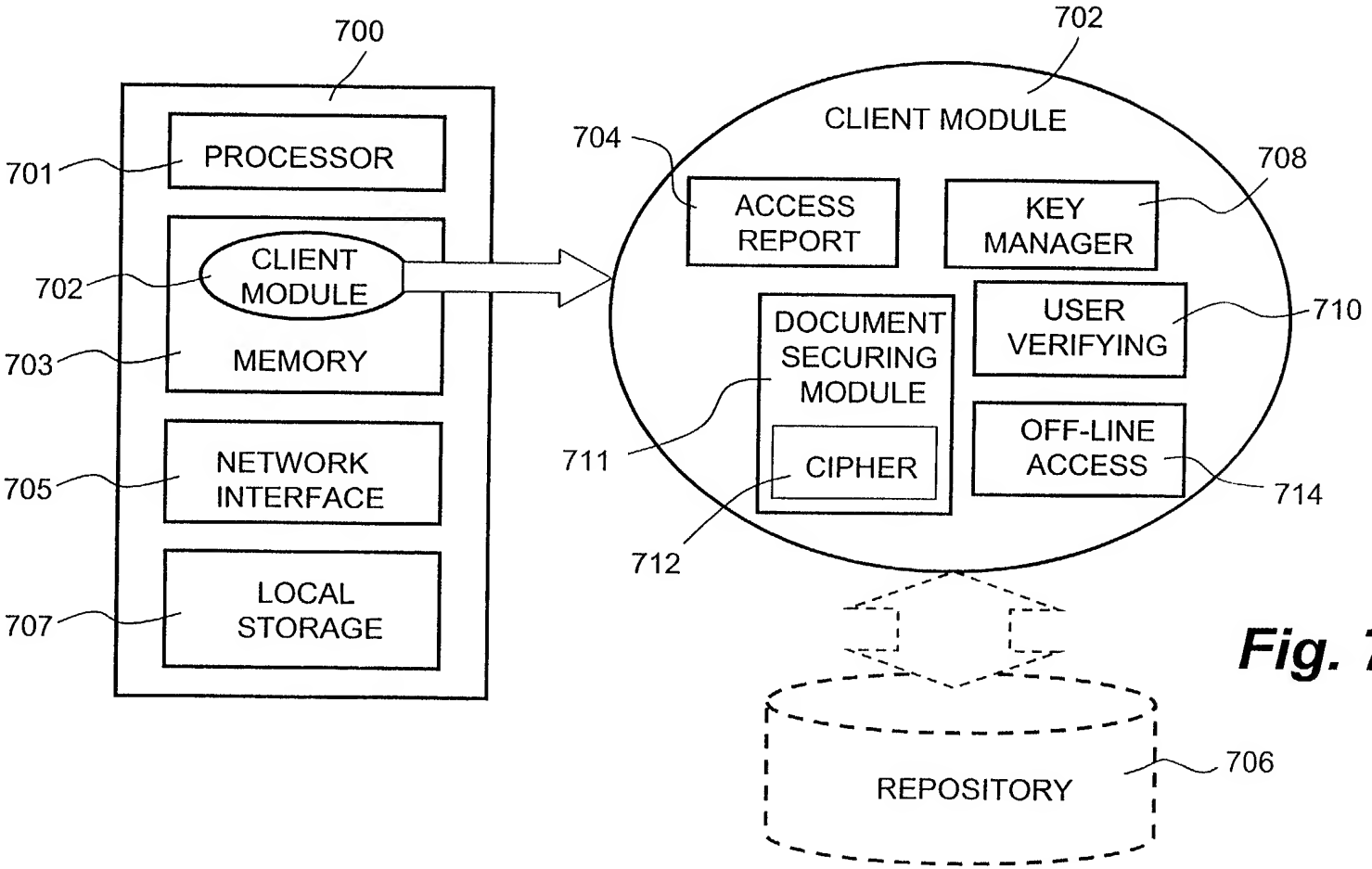

700
PROCESSOR
701
CLIENT MODULE
702
MEMORY
703
NETWORK INTERFACE
705
LOCAL STORAGE
707
702
CLIENT MODULE
704
ACCESS REPORT
KEY MANAGER
708
DOCUMENT SECURING MODULE
711
CIPHER
712
USER VERIFYING
710
OFF-LINE ACCESS
714
REPOSITORY
706

Fig. 7A

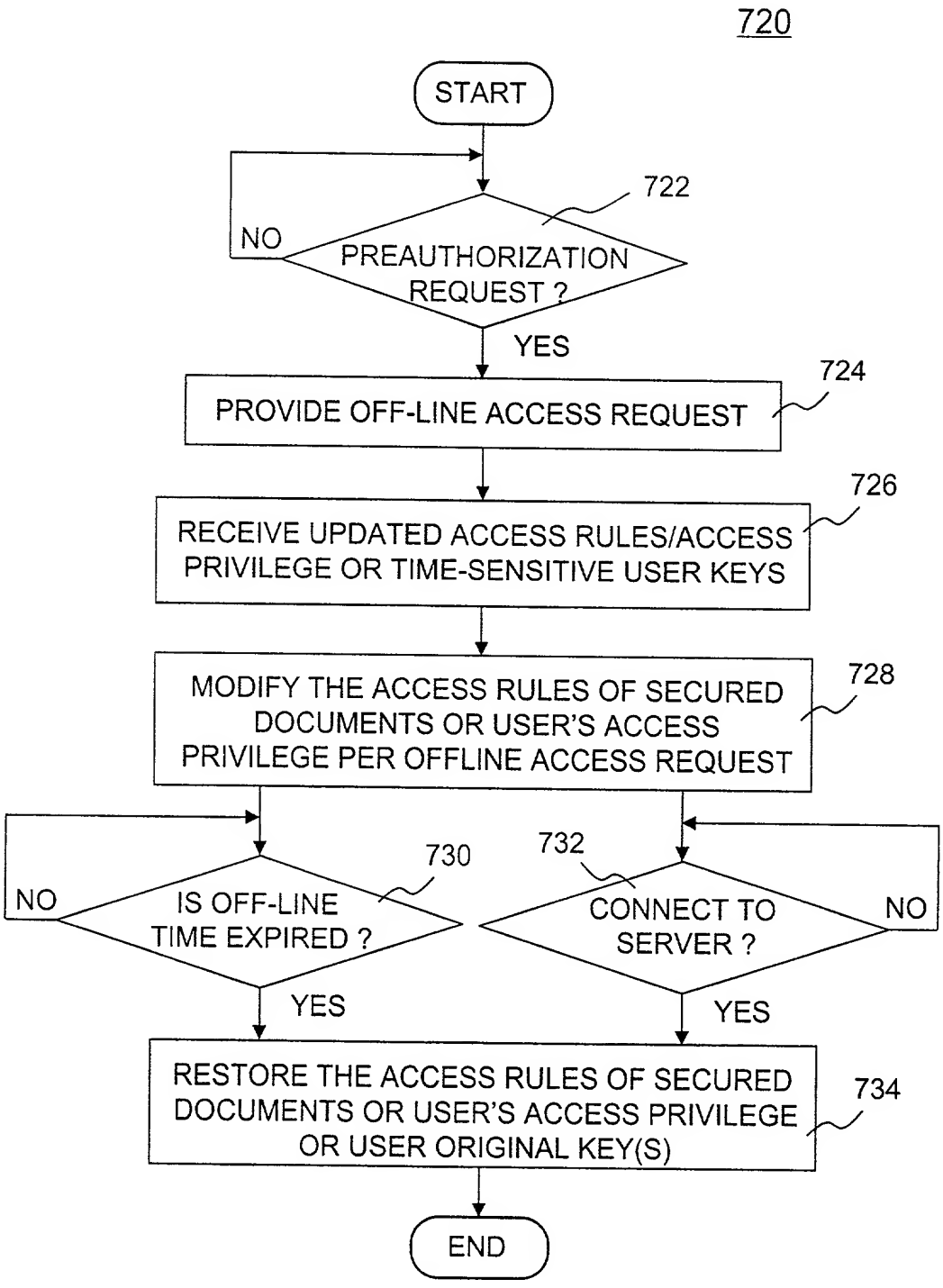

720
START
722
NO
PREAUTHORIZATION REQUEST ?
YES
724
PROVIDE OFF-LINE ACCESS REQUEST
726
RECEIVE UPDATED ACCESS RULES/ACCESS PRIVILEGE OR TIME-SENSITIVE USER KEYS
728
MODIFY THE ACCESS RULES OF SECURED DOCUMENTS OR USER'S ACCESS PRIVILEGE PER OFFLINE ACCESS REQUEST
730
NO
IS OFF-LINE TIME EXPIRED ?
YES
732
CONNECT TO SERVER ?
NO
YES
734
RESTORE THE ACCESS RULES OF SECURED DOCUMENTS OR USER'S ACCESS PRIVILEGE OR USER ORIGINAL KEY(S)
END

Fig. 7B

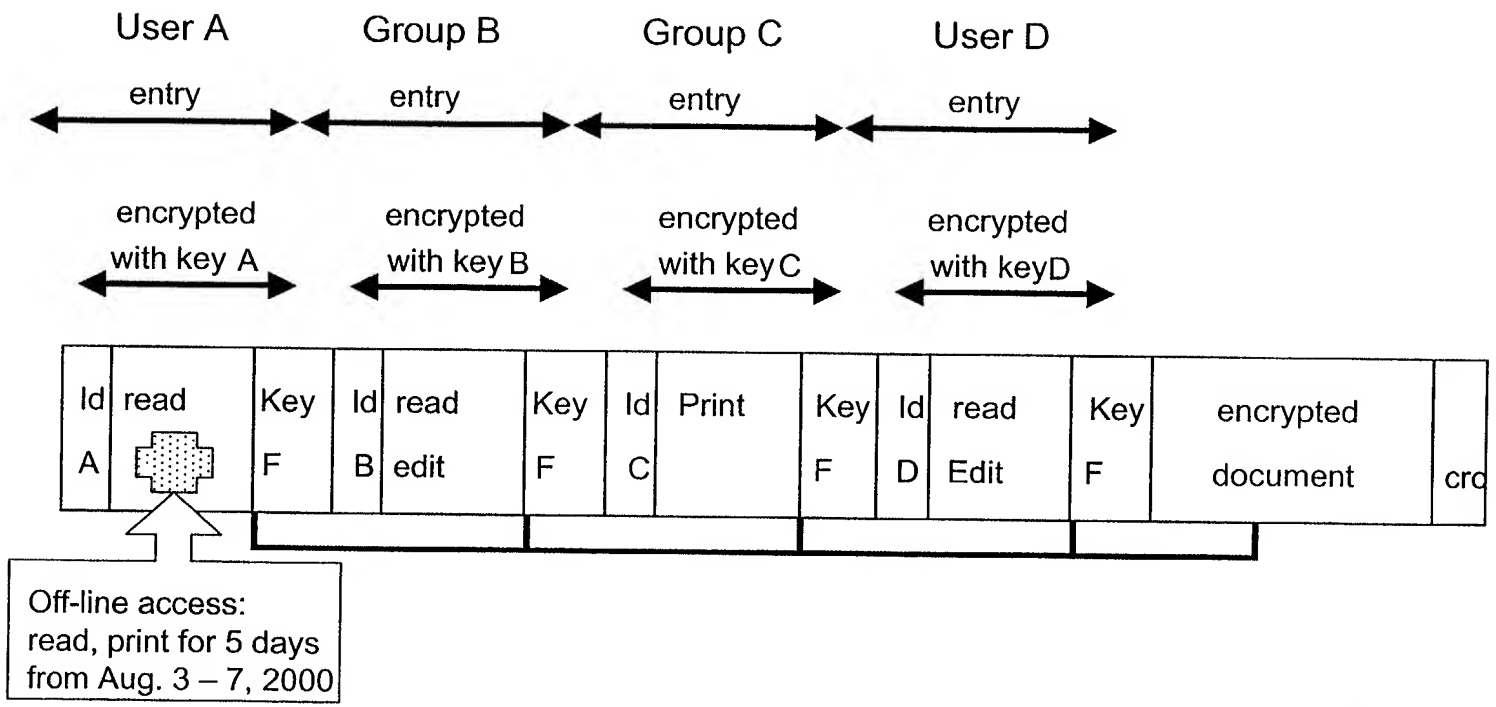

User A
Group B
Group C
User D
entry
entry
entry
entry
encrypted with key A
encrypted with key B
encrypted with key C
encrypted with keyD
Id A
read
Key F
Id B
read edit
Key F
Id C
Print
Key F
Id D
read Edit
Key F
encrypted document
crc
Off-line access:
read, print for 5 days
from Aug. 3 – 7, 2000

Fig. 7C